An Enhanced View of Incidence Functions for Applying Graph Theory to Modeling Network Intrusions

CHUCK EASTTOM, MO ADDA,
School of Computing
University of Portsmouth
Portsmouth, Hampshire, UK

Abstract: - Graph theory provides a robust tool for modeling a diverse range of subjects. It has been widely applied to computer networks and even network attacks. However, the incidence function in graph theory is often given a cursory treatment. This current research involves applying a range of information theory equations to describe the incidence function in a graph of a computer network. This improves modeling of computer network attacks and intrusions. Specifically attacks that involve substantial changes in network traffic can be more accurately modeled, if the incidence function of the graph is expanded.

Key-Words: - Graph theory, Shannon entropy, Rényi entropy, incidence functions, information theory

Received: April 8, 2020. Revised: June 9, 2020. Accepted: June 16, 2020. Published: June 18, 2020

1 Introduction

Graph theory is widely used to model a variety of activities. It has been a core part of engineering and network modeling for many years [1] [2] [3]. Graph theory has also been applied to such disparate topics as neurological degenerative diseases [4] and analysis of stocks [5].

Various aspects of graph theory, including algebraic graph theory have been explored for modeling a diverse range of subjects [6]. Graph theory has been utilized with linear algebra to understand systems based on the graphs incidence matrix [7] [8] and degree matrix [9].

Many researchers have found that understanding the Laplacian of a graph is also informative for understanding the system being modeled. The Laplacian matrix is usually defined as the degree matrix minus the adjacency matrix [11]. The Laplacian matrix is also referred to as the admittance matrix, Kirchhoff matrix, or discrete Laplacian. The Laplacian is sometimes normalized as shown in equation 1.

$$\mathcal{L}_{i,j}(G) = \begin{cases} 1 & \text{if } i = j \text{ and } d_j \neq 0 \\ -\dfrac{1}{\sqrt{d_i\, d_j}} & \text{if } i \text{ and } j \text{ are adjacent} \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

Calculating the graphs Laplacian leads to other information from algebraic graph theory. As one example, Kirchhoff's theorem states that the determinant of the Laplacian of a graph indicates number of spanning trees in a graph [12]. A spanning tree T of an undirected graph G is a subgraph that is a tree which includes all of the vertices of G, with minimum possible number of edges [13]. By first calculating the graphs Laplacian, additional data immediately follows, such as using the Laplacians determinant to gain information about spanning trees in that graph. This is one example of the breadth and depth of research in applying algebraic graph theory to various modelling problems. The existing body of graph theory research provides a rich set of mathematical tools for analysing many phenomena, including network intrusions. This current work does not refute the existing body of research, but rather seeks to add to it.

What is missing from the literature is an exploration of the incidence function. An incidence function is normally defined as a function that maps every edge to a pair of vertices, either ordered or unordered [14] [15]. While other aspects of graph theory have an extensive corpus of research exploring them, incidence functions have sparse research. This is particularly interesting when using graph theory for modelling network traffic, or computer network intrusions. Merely having two or more vertices connected by an incidence function is interesting but knowing the specific nature of that connection would be more useful. Thus, understanding the incidence function is quite important.

In network traffic, it is not accurate to simply state two network nodes, or vertices, are connected. Understanding the nature of that connection is

essential. For example, it can be useful to understand the nature of the data flowing between the two vertices, as well as the amount of data. Therefore, expanding the incidence function to include more rigorous descriptions would improve the ability to model networks and network attacks utilizing graph theory.

The current literature and research does not adequately explore incidence functions. Incidence functions are mentioned as simply the connection between two vertices. The specific nature of the connection is not explored. This current study explores the actual function that connects two or more edges.

2 Problem Formulation

There is a gap in the literature regarding the exploration of incidence functions as they relate to specific modeling problems with graph theory. While other aspects of graph theory have an extensive amount of research, incidence functions is an overlooked area. A better understanding of incidence functions will lead to more information being derived from modeling real-world systems with graph theory.

There is a need to expand the examination of the incidence function. A better understanding of the function that connects the vertices, will improve the accuracy and efficacy of graph theory modeling of systems. The particular focus in this current study is the application of graph theory to modeling computer network intrusions and attacks. There is existing research on modeling networks and network intrusions with graph theory [16] [17]. However, those attempts have not expanded the examination of the incidence function. This current study will expand the examination of the incidence function when applying graph theory to modeling network intrusions.

3 Problem Solution

Given the current study is directed towards application of graph theory to computer intrusions it is an important first step to understand the nature of network traffic. Ultimately, such traffic is information. Whether that data is transmitted via radio waves, electrical signal in unshielded twisted pair cable, or some other media, the traffic is information. Even malicious traffic is information. Therefore, a logical place to begin expanding the incidence function would be to integrate information theory into incidence functions. The solution posited in this paper is to include the concepts of information theory to describe the incidence function between vertices in a computer network graph, in general, emphasizing in particular on intrusions.

There have been some attempts to incorporate small portions of information theory into narrowly defined specific applications of computer network traffic analysis [18 [19]. However, these attempts have been very narrowly focused and do not include graph theory, The goal of this work is to expand upon existing research that utilizes graph theory to understand computer networks, by incorporating a spectrum of information theory techniques into graph theory. The information theory functions serve as the incidence functions for the graph of the intrusion. This will provide a more robust tool for understanding computer networks that currently exists in the literature.

The current study posits that the incidence function is one or more information theory equations. Rather than simply state that the incidence function connects two or more vertices via their edges or arcs, the connection between vertices is a measurement of the information flow between the vertices. The vertices are connected via information. That information flow is quantified either via the amount of information (Shannon Entropy) or the diversity of information (various diversity indices).

3.1 Shannon Information

A logical place to begin is with integrating Shannon information into graph theory. This metric was first proposed by Claude Shannon and was intended to quantify the information content present in a particular text string. The value is referred to as information entropy. Essentially, the informational content of a message is that message's entropy p_i denotes the proportion of symbols which belong to the to the *i*th class of character in the string being examined [20]. information entropy is expressed as shown in equation 2.

$$H' = -\sum_{i=1}^{n} p_i * \ln(p_i) \qquad (2)$$

This value can be readily integrated into incidence functions. An incidence function maps edges to pairs of vertices. In the case of a computer network, the vertices would be nodes on the network. What flows between them is information. Quantifying how much information is flowing between to vertices provides a better understanding of the network. This is true for analyzing network

traffic or for analyzing intrusions. A Denial of Service attack, as one example, would yield a sudden and substantial increase in information flowing between nodes. This fact will be explored later in this paper with a specific case study and a laboratory experiment.

Understanding the change in flow of information would provide a better understanding of the attack. The volume of traffic varies with different DoS attacks. Thus, the Shannon Information or Shannon Entropy can provide insight into the nature of the DoS attack.

3.2 Simpson Index

The Simpson index was introduced in 1949 by Edward H. Simpson to measure the degree of concentration of individuals of a specific category. When this is applied in economics, it is referred to as Herfindahl index or the Herfindahl–Hirschman index. The Simpson index equals the probability that two entities taken at random from the dataset of interest represent the same class or type of entities [21], as shown in equation 3.

$$\lambda = \sum_{i=1}^{R} p_i^2, \tag{3}$$

In equation 3, *R* is the total number of types or classes in the dataset. This is referred to as the richness of the dataset. This equation is also equal to the weighted arithmetic mean of the proportional abundances p_i of the types of interest, with the proportional abundances themselves being used as the weights. One could use either the Simpson index, or the Shannon entropy separately to understand what connects two vertices in a computer network. However, it may be advantageous to consider both metrics. This would make the incidence function between the two vertices, a system of two equations.

In the case of a Denial of Service attack, the information flow should increase dramatically, but the diversity of the data should reduce. This is due to many DoS attacks being predicated on a flood of a specific type of packet [22] [23].

Thus, when graphing a network, a sudden increase in both Shannon entropy and a decrease in the Simpson index would be indicative of a DoS attack. This is only one example. A large data exfiltration would have similar characteristics but would be a) less volume and b) fewer vertices (network nodes) involved. Berba's study in 2019 clearly demonstrated the substantial spike in traffic from a single IP and of a single protocol that indicated data exfiltration [24].

3.3 Shannon-Weaver Index

A metric related to Simpson index is the Shannon-Weaver index. This metric quantifies the concentration of individuals that are classified into groups [25]. The formula is shown in equation 4.

$$H = -\sum_{i=1}^{s} p_i \ln p_i \tag{4}$$

S is the quantity of individual species found in the community being studied. The p_i is still the proportion of symbols that are part of the *i*th category of symbol in the text string of interest, similar to Shannon entropy formulation.

There are a several variants of the Simpson index. Two examples of such variations are the Berger–Parker index, the Inverse Simpson index, the Dominance index, and the Gini-Simpson index. All of these variations are directed towards studying how one particular class of items compare to the entirety of items. As with the Simpson index, when applied to computer networks, this can be indicative of DoS attacks, data exfiltration, or other types of network attacks [26], [27], [28].

An example of how DoS attacks affect network traffic is found in 2018. On November 13, 2018 several internet service providers in Cambodia were attacked with a large-scale distributed Denial of Service attack. The average attack size per IP prefix was 2.48Gbps [29]. In a worst-case scenario, an attack of this size spread across 38 IP prefixes is potent enough to overwhelm a 10Gbps ISP line. The attack was a UDP (User Datagram Packet) flood on random ports [30]. The attack targeted more than 80 subnets for six hours. At its peak the bandwidth utilized was 150 Gbps [31].

In 2017 the mean bandwidth in Cambodia was 13 mbps [32]. Figure 1 demonstrates the actual impact on bandwidth of this attack.

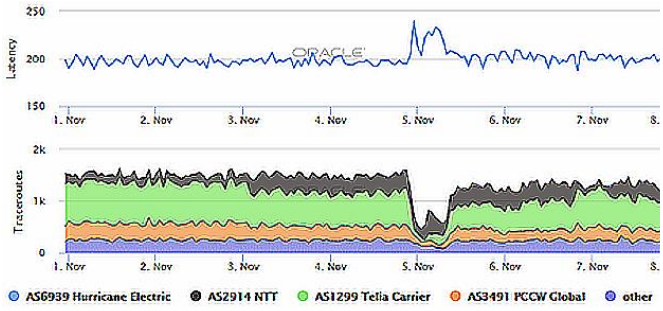

Fig. 1

The top portion of figure 1 shows packet latency and the bottom shows traceroutes. During the actual attack, latency increased substantially and the number of traceroutes that did not time out decreased substantially. These are tell-tale signs of a Denial of Service attack.

The bandwidth utilization for the Cambodia Network Exchange fluctuates between 2 Gbps and 20 Gbps, throughout the day [33]. Getting precise data for Cambodia internet usage is simply not possible as such data is not published.

Clearly the percentage of UDP traffic dramatically increased during the attack, thus altering the Shannon Entropy. Furthermore, rather than the normal distribution of protocols in network traffic, the traffic during the attack was overwhelmingly UDP which would also affect all of the diversity indices. A specific laboratory experiment demonstrating the details of these effects is provided later in this paper.

3.5 Hartley Entropy

Hartley entropy was introduced by Ralph Hartley in 1928, and thus predates Shannon's work on information theory. This is often simply called the Hartley function. If a sample from a finite set A uniformly at random is picked, the information revealed after the outcome is known is given by the Hartley function, shown in equation 5 [34].

$$H_0(A) := \log_b |A| \tag{5}$$

In equation 4, |A| denotes the cardinality of A. If the base of the logarithm is 2, then the unit of uncertainty is now referred to as the Shannon. If it is the natural logarithm, then the unit is the nat. Hartley used a base-ten logarithm, and with this base, the unit of information is called the Hartley in his honour.

Like the Shannon-Weaver and Simpson indices, the Hartley entropy provides insight regarding the diversity in a given dataset. Substantial and sudden changes in the diversity of network traffic can be indicative of several different network attacks including DoS attacks and data exfiltration.

3.6 Rényi entropy

Related to some of the previous entropy values discussed so far is the Rényi entropy. The Rényi entropy generalizes the Hartley entropy, the Shannon entropy, the collision entropy and the min-entropy [35], as shown in equation 6.

$$\mathrm{H}_\alpha(X) = \frac{1}{1-\alpha} \log \left(\sum_{i=1}^{n} p_i^\alpha \right) \tag{6}$$

In equation 5, X is a discrete random variable with possible outcomes (*1, 2, …., n*) and corresponding probabilities p_i for $i = 1$ to n. Since this metric is generally used in information theory, the logarithm is typically base 2, and the order, α , is $0 < \alpha < 1$.

The Rényi entropy is a measure of the diversity in a dataset. The Rényi entropy is also important in quantum information, where it can be used as a measure of entanglement. As with other diversity metrics, this can be useful in fully understanding the data flow between two or more network nodes.

3.7 Synthesizing the metrics

The goal of incorporating information theory with graph theory is to provide a more robust modeling tool. In the current study the focus is on applications in computer networks including computer network intrusions. However, this process can be applied to any system that involves information.

The issue addressed in this current study is to expand on what is currently considered regarding incidence functions. All too often the incidence function is simply discussed as a connecting two vertices via an edge or arc [36], [37], [38]. It is commonplace in the literature to provide no further details on the incidence function. Expanding the definition of the incidence function to include the information flowing between two vertices adds detail to graphs that model any information related network.

When considering two network nodes, the connection between them is an information flow. Examining that flow is critical to fully understanding the network itself. The methods

posited in this section are not mutually exclusive. Rather, they are a set of tools that can be utilized as needed in the specific situation.

3.8 A Case Study

Detailed specifics are not available on most actual DoS attacks. Published case studies generally provide information regarding peak bandwidth utilization, but not details such as the distribution of protocols in network traffic, or a granular view of the changes in network traffic [39], [40], [41], [42]. Therefore, a laboratory network was established with typical network services and simulated user traffic, then that network was subjected to a typical Denial of Service attack. By using a laboratory environment, all the details of the traffic could be captured, and the equations posited in this study could be fully tested.

The lab was setup with a Linux server running Ubuntu 19.4 and common services [43], [44], [45], [46]. There were four client virtual machines setup. Two where running Windows 10 and 2 running Ubuntu 19.4. The clients were used for typical network activities such as visiting web sites, DNS lookups, and email. Traffic was measured with Wireshark. The arithmetic mean of traffic by protocol is shown in table 1.

Table 1 Network Protocols

Port	Protocol	Mean % of Traffic	TCP/UDP
20/21	FTP	4%	TCP
53	DNS	32%	UDP
80	HTTP	16.5%	TCP
443	HTTPS	30.5%	TCP
465	SMTPS	6.5%	TCP
995	POP3S	9.5%	TCP

Table 1 describes the specific protocols that were in operation on the test network. The percentage of traffic used by each protocol is provided. The mean total bandwidth was 2.5 mbps. After establishing a lab environment and running typical network traffic, the next step was to evaluate the content of this traffic utilizing the equations posited in this study. The results of the calculations are shown in table 2.

Table 2 Values before Attack

Equation	Value
Shannon Entropy	0.323
Simpson Index	.765
Shannon Weaver Index	1.57
Rényi entropy	-0.02

For the Rényi entropy a α value of .32 was utilized. This is due to the fact that as α approaches zero, the Rényi entropy increasingly weighs all possible events more equally. That is not appropriate with network traffic. Therefore, a α value was used equal to the largest probability for a single packet type. Once these statistics were calculated the next step was to execute a Denial of Service attack on the network. To accomplish this a UDP flood was executed on the network using a bandwidth of 10 mbps. This altered the distribution of protocols. The distribution during attack is shown in Table 3.

Table 3 Traffic Flow During Attack

Port	Protocol	Mean % of Traffic	TCP/UDP
20/21	FTP	0.5%	TCP
53	DNS	5%	UDP
80	HTTP	2.5%	TCP
443	HTTPS	4.5%	TCP
465	SMTPS	1%	TCP
995	POP3S	1.5%	TCP
80	UDP FLOOD	85.5%	UDP

The change in traffic flow also changed the entropy and diversity calculations. The new values are shown in table 4.

Table 4 Values During Attack

Equation	Value
Shannon Entropy	0.5315
Simpson Index	0.2807
Shannon Weaver Index	0.65
Rényi entropy	-0.09

Given that during the attack the probability of the traffic being UDP flood was dramatically increased an α value equal to the probability of UDP flood traffic was used, .855. This is also consistent with the values used for the pre-attack calculations.

The results of the experiment demonstrate that the Shannon Entropy increased by 64.55%. The Simpson Index decreased by 63.31%. The Shannon Weaver Index decreased by 58.6%. The Rényi entropy decreased by 350%. The information content increased significantly, while all diversity indices decreased significantly. This indicates that using these equations provides an understanding of a flood-based Denial of Service attack.

4 Conclusion

This paper provides an outline to apply information theory to more fully understanding the incidence functions in graph theory. As graph theory is

routinely used in a wide range of modeling applications, this work can enhance such applications. Equations from information theory quantify the connection between vertices, and thus are the incidence functions.

A range of information theory metrics including the Simpson index, Shannon entropy, and Rényi entropy were proposed as possible incidence functions when applying graph theory to computer networks. It must also be noted that these metrics can be used in combination to understand not only the flow of information, but also the diversity in that flow.

This work can be expanded by including rates of change for both information and information diversity. Partial differential equations are already applied with thermodynamic entropy. Shannon himself created differential entropy but was incorrect in his equation. Limiting density of discrete points is a technique created by Edwin Jaynes to correct issues with Claude Shannon's differential entropy formula. It would be of interest to explore utilizing this function, or some similar equation, for the incidence function in graph theory.

In addition to expanding the incidence function, other aspects of algebraic graph theory should be explored for applications in analyzing network traffic. Spectral graph theory and fractional graph theory are obvious areas to explore. Specialized matrices such as Jacobian matrices are also areas that should be explored in future studies.

While the current study is directed to studying computer networks, information theory can be integrated into graph theory in other modeling contexts. For example, consider the previously mentioned neurological applications of graph theory. Viewing signals between neurons as information would provide additional data on the neurological structures being studied. In the case of degenerative neurological disorders, one would expect to see a reduction in the information flow.

References:

[1] N. Deo, Graph Theory with Applications to Engineering and Computer Scienc. Dover Publications. 2017 .

[2] Dörfler F, Simpson-Porco JW, Bullo F. Electrical networks and algebraic graph theory: Models, properties, and applications. Proceedings of the IEEE Vol.106, No. 5, pp. 977-1005. 2018.

[3] Rangaswamy KD, Gurusamy M. Application of Graph Theory Concepts in Computer Networks and its Suitability for the Resource Provisioning Issues in Cloud Computing-A Review. JCS. Vol., pp. 163-72. 2018.

[4] F. Agosta, S. Sala, P. Valsasina, A. Meani, E. Canu, G. Magnani, ... & A. Fali Brain network connectivity assessed using graph theory in frontotemporal dementia Neurology, Vol. 81, Issue. 2, pp. 134-143. 2013.

[5] Li W, Zhao X. Multiscale horizontal-visibility-graph correlation analysis of stock time series. EPL (Europhysics Letters).Vol. 3, No. 122. 2018.

[6] C. Godsil & G. Royle. Algebraic graph theory. Springer Science & Business Media. 2013.

[7] Wang Y, Zhang N, Kang C, Kirschen DS, Yang J, Xia Q. Standardized matrix modeling of multiple energy systems. IEEE Transactions on Smart Grid. Vol. 10, Issue 1, pp. 257-70. 2017.

[8] van der Schaft A. Modeling of physical network systems. Systems & Control Letters. Vol. 101, pp. 21-7. 2017.

[9] Reinisch EC, Cardiff M, Feigl KL. Graph theory for analyzing pair-wise data: application to geophysical model parameters estimated from interferometric synthetic aperture radar data at Okmok volcano, Alaska. Journal of Geodesy. Vol. 91, No. 1, pp.:9-24. 2017.

[10] Dong X, Thanou D, Frossard P, Vandergheynst P. Learning Laplacian matrix in smooth graph signal representations. IEEE Transactions on Signal Processing. Vol. 64, No. 23, pp. 6160-73. 2016.

[11] F. Meyer & X. Shen. Perturbation of the eigenvectors of the graph Laplacian: Application to image denoising. Applied and Computational Harmonic Analysis. Vol. 36, No.2, pp. 326-334. 2014.

[12] J. Huang & S. Li. On the normalized Laplacian spectrum, degree-Kirchhoff index and spanning trees of graphs. Bulletin of the Australian Mathematical Society. Vol. 91, No. 3, pp. 353-367. 2015.

[13] J. Gross, J. Yellen, & P. Zhang. Handbook of graph theory. Chapman and Hall/CRC. 2013.

[14] Trudeau, R.J., Introduction to graph theory. Courier Corporation. 2013

[15] Chartrand G, Zhang P. A first course in graph theory. Courier Corporation. 2013.
[16] C. Easttom A Systems Approach To Indicators Of Compromise Utilizing Graph Theory. IEEE International Symposium on Technologies for Homeland Security. 2018.
[17] C. Easttom On the Application of Algebraic Graph Theory to Modeling Network Intrusions. IEEE 10th Annual Computing and Communication Conference. 2020.
[18] Behal S, Kumar K. Detection of DDoS attacks and flash events using novel
[19] information theory metrics. Computer Networks. Vol. 116, pp. 96-110. 2017.
[20] Zhao JW. A Novel Method for Predicting Network Traffic Based on Maximum Entropy Principle. International Journal of Future Generation Communication and Networking. Vol. 9, No. 1, pp. :97-106. 2016.
[21] Easttom, C. Modern Cryptography. Applied mathematics for encryption and information security. McGraw-Hill Publishing. 2015.
[22] Idhammad M, Afdel K, Belouch M. Dos detection method based on artificial neural networks. International Journal of Advanced Computer Science and Applications. Vol. 8, No. 4, pp. 465-71. 2017.
[23] Wong F, Tan CX. A survey of trends in massive DDoS attacks and cloud-based mitigations. International Journal of Network Security & Its Applications. Vol 6, No. 3, pp. 57. 2014.
[24] Berba, P. Data Analysis for Cyber Security 101: Detecting Data Exfiltration. Retrieved from https://towardsdatascience.com/data-analysis-for-cybersecurity-101-detecting-data-exfiltration-ae887594f675. 2019.
[25] Matta G, Gjyli L, Kumar A, Machel J. Hydrochemical characteristics and planktonic composition assessment of River Henwal in Himalayan Region of Uttarakhand using CPI, Simpson's and Shannon-Weaver Index. Journal of Chemical and Pharmaceutical Sciences. Vol. 11, No. 1, pp. 122-30. 2018.
[26] Durkota K, Lisý V, Kiekintveld C, Horák K, Bošanský B, Pevný T. Optimal strategies for detecting data exfiltration by internal and external attackers. In International Conference on Decision and Game Theory for Security. pp. 171-192. Springer, Cham. 2017.
[27] Bukac V, Matyas V. Analyzing traffic features of common standalone dos attack tools. In International Conference on Security, Privacy, and Applied Cryptography Engineering.pp. 21-40. Springer, Cham. 2015.
[28] Basicevic I, Ocovaj S, Popovic M. Use of Tsallis entropy in detection of SYN flood DoS attacks. Security and Communication Networks. Vol. 8, No. 18, pp. 3634-40. 2015.
[29] Mitchell R.. DDoS tsunami: A Cambodian case study. Retrieved from https://blog.apnic.net/2019/06/25/ddos-tsunami-a-cambodian-case-study/. 2019.
[30] Cimpanu, C. Cambodia's ISPs hit by some of the biggest DDoS attacks in the country's history. Retrieved from https://www.zdnet.com/article/cambodias-isps-hit-by-some-of-the-biggest-ddos-attacks-in-the-countrys-history/ 2018.
[31] Pascu, L. DDoS attack on Cambodia’s top ISPs reached 150Gbp. Retrieved from https://securityboulevard.com/2018/11/ddos-attack-on-cambodias-top-isps-reached-150gbps/. 2018.
[32] United Nations. Leveraging Investments in Broadband for National Development: The Case of Cambodia. Retrieved from http://unohrlls.org/custom-content/uploads/2019/02/Cambodia-Broadband-Case-Study-UNOHRLLS-2018.pdf. 2018.
[33] Cambodia internet statistics https://www.peeringdb.com/ix/1209 2019.
[34] Hsue WL, Chang WC. Real discrete fractional Fourier, Hartley, generalized Fourier and generalized Hartley transforms with many parameters. IEEE Transactions on Circuits and Systems I: Regular Papers. Vol. 62, No. 10, pp. 2594-605. 2015 Acharya J, Orlitsky A, Suresh AT, Tyagi H. Estimating Rényi entropy of discrete distributions. IEEE Transactions on Information Theory. Vol. 63, No. 1, pp. 38-56. 2016.
[35] Guariglia E. Entropy and fractal antennas. Entropy. Vol. 18, No. 3, pp. 84. 2016.

[36] Han L, Liu G, Yang X, Han B. A Computational Synthesis Approach of Mechanical Conceptual Design Based on Graph Theory and Polynomial Operation. Chinese Journal of Mechanical Engineering. Vol. 33, No. 1, pp. 2. 2020.
[37] Goldreich O. Flexible models for testing graph properties. In Electronic Colloquium on Computational Complexity (ECCC). Vol. 25, pp. 104. 2018.
[38] Marzuki CC. Total irregularity strength of m-copies of rhombus graph. In Journal of Physics: Conference Series. Vol. 1116, No. 2, pp. 022023. 2018.
[39] Yan Q, Yu FR, Gong Q, Li J. Software-defined networking (SDN) and distributed Denial of Service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. IEEE communications surveys & tutorials. Vol.18, No. 1. pp. 602-22. 2015.
[40] Yu J. An empirical study of Denial of Service (DoS) against VoIP. In2016 15th International Conference on Ubiquitous Computing and Communications and 2016 International Symposium on Cyberspace and Security (IUCC-CSS). pp. 54-60). IEEE. 2016.
[41] Kang MS, Gligor VD, Sekar V. Defending against evolving ddos attacks: A case study using link flooding incidents. In Cambridge International Workshop on Security Protocols. pp. 47-57. Springer, Cham. 2016.
[42] Šimon M, Huraj L, Horák T. DDoS Reflection Attack Based on IoT: A Case Study. In Computer Science On-line Conference.pp. 44-52. Springer, Cham. 2018.
[43] Jang MH, Messier R. Security strategies in Linux platforms and applications. Jones & Bartlett Publishers; 2017.
[44] Gebali F. Analysis of computer networks. Cham: Springer International Publishing. 2015.
[45] Robertazzi TG. Introduction to computer networking. Springer. 2017.
[46] Sunshine CA, editor. Computer network architectures and protocols. Springer Science & Business Media. 2013.